Digital Signature Verification System Using Convolutional Neural Networks

Aman Kumar Mishra
Department - Information Technology
Greater Noida Institute of Technology (Engineering Institute)
Gautam Buddh Nagar, India
Dr.Shivani Dubey
Department - Information Technology
Greater Noida Institute of Technology (Engineering Institute)
Gautam Buddh Nagar, India
dubey.shivani@gmail.com
Prof.Vikas Singhal
Department - Information Technology
Greater Noida Institute of Technology (Engineering Institute)
Gautam Buddh Nagar, India
vikassinghal75@gmail.com
Dr.Pankaj Gupta
Department - Information Technology
Greater Noida Institute of Technology (Engineering Institute)
Gautam Buddh Nagar, India
Drpkg03@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.11/Issue01/JAAE10092
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue01/JAAE10092
Received: 03, January 2024 | Revised:10, January 2024 | Accepted: 19, January 2024 | Published Online: 24, January 2024
https://www.ijirae.com/volumes/Vol11/iss-01/01.JAAE10092.pdf
Article Citation: Aman,Shivani,Vikas,Pankaj(2024).Digital Signature Verification System Using Convolutional Neural Networks. IJIRAE::International Journal of Innovative Research in Advanced Engineering, Volume 11, Issue 01 of 2024 pages 01-07. **Doi:>** https://doi.org/10.26562/ijirae.2024.v1101.01
BibTeX Aman2024@Digital
Academic Editor-Chief: Dr.A.Arul Lawrence Selvakumar, AM Publications, India

Abstract: The design, development, and evaluation of a signature verification system, a critical component of biometric authentication. The study employs two primary datasets, the MCYT (MasterCard Young Teenager) Signature Dataset and the GPDS (Greek Sign Language Recognition) Signature Dataset, to assess the system's adaptability and accuracy. The MCYT dataset, featuring 6600 signature samples, provides variability in writing styles and demographic information for potential nuanced analyses. In contrast, the GPDS dataset, comprising 4000 signatures, introduces dynamic signing variations during Greek Sign Language communication. The project aims to develop a robust signature verification system capable of handling diverse scenarios, ultimately contributing to the advancement of biometric technology. The research combines insights from real-world variability and linguistic nuances, offering a comprehensive understanding of the system's effectiveness.

Keywords: Digital Signature, Verification System, Convolutional Neural Networks, Image Processing

I. INTRODUCTION

In the rapidly evolving landscape of biometric authentication, the development and implementation of effective signature verification systems have become increasingly paramount. This project report is dedicated to exploring, designing, and evaluating a signature verification system that strives to transcend conventional methodologies. Signature verification, as a facet of biometrics, plays a pivotal role in secure authentication processes across various domains, including finance, legal documentation, and access control. The purpose of this project is to address the complexities inherent in signature authentication, leveraging advanced technologies such as Digital Signal Processing (DSP) and neural networks. The report aims to provide a comprehensive understanding of the theoretical foundations, methodologies employed, and the practical implications of deploying a signature verification system. By focusing on two key datasets, the MCYT (MasterCard Young Teenager) Signature Dataset and the GPDS (Greek Sign Language Recognition) Signature Dataset, this project seeks to capture the nuances and challenges associated with real-world signatures and dynamic signing variations. Through an in-depth exploration of these datasets and the subsequent development of a robust signature verification system, this project endeavors to contribute valuable insights to the broader field of biometric technology.

- **The Significance of Signature Verification:**
  In contemporary society, where secure and efficient authentication mechanisms are essential, signature verification stands out as a fundamental biometric method.
  Traditionally, signatures have served as unique identifiers, playing a crucial role in validating the authenticity of individuals on legal documents, financial transactions, and access control systems. The reliance on signatures necessitates the development of sophisticated verification systems capable of discerning genuine signatures from forgeries accurately.
- **Challenges in Signature Verification:**
  While the use of signatures for authentication is prevalent, it comes with inherent challenges. Variability in writing styles, environmental conditions during signature capture, and the potential for forgery pose significant hurdles. Traditional methods often struggle to adapt to these challenges, prompting the exploration of advanced technologies to enhance the accuracy and reliability of signature verification systems.

Technological

- **Advancements:**
  The advent of Digital Signal Processing (DSP) and neural network technologies has ushered in a new era for signature verification. DSP techniques enable the extraction of intricate features from signature data, enhancing the system's ability to differentiate between genuine and forged signatures. Concurrently, neural networks, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable capabilities in image recognition tasks, making them well-suited for signature analysis.
- **Project Objectives:**
  The primary objectives of this project are threefold: first, to understand the theoretical underpinnings of signature verification, exploring its historical context, challenges, and the need for advanced methodologies; second, to delve into the practical application of DSP and neural networks, specifically CNNs, in the development of a signature verification system; and third, to evaluate the system's performance using two prominent datasets, MCYT and GPDS, representing diverse scenarios and linguistic nuances.
- **Dataset Selection and Characteristics:**
  The MCYT Signature Dataset, a comprehensive collection of 6600 signatures from 330 individuals, offers a rich array of genuine and forgery samples. The dataset's variability, with signatures captured using different devices and under various conditions, mirrors real-world scenarios. Moreover, the inclusion of demographic information provides an additional layer of complexity for potential demographic-centric analyses. Complementing the MCYT dataset, the GPDS Signature Dataset introduces a distinctive challenge. With 4000 signatures, including 2000 genuine and 2000 forgery samples, the dataset focuses on signatures expressed during Greek Sign Language communication. This not only poses challenges related to dynamic signing variations but also adds a linguistic context, contributing to the system's adaptability in diverse communication scenarios.
- **Theoretical Foundations:**
  Before delving into the practical aspects of the project, it is crucial to establish a solid theoretical foundation. Signature verification, as a biometric method, has a rich historical context. Early forms of signature analysis relied on manual comparison, a subjective and often error-prone process. The advent of computer-based methods brought forth automated signature verification systems, leading to a paradigm shift in authentication technology.
- **Digital Signal Processing (DSP) in Signature Verification:**
  DSP techniques play a pivotal role in signature verification by extracting relevant features from signature data. The process involves capturing and processing signature images, converting them into digital signals for analysis. Key DSP applications include noise reduction, feature extraction, and the enhancement of relevant signature characteristics. These techniques contribute to the system's ability to discern genuine signatures from forgeries in the presence of variability and environmental factors.
- **Neural Networks in Signature Verification:**
  The integration of neural networks, particularly Convolutional Neural Networks (CNNs), signifies a significant advancement in signature verification technology. CNNs are well-suited for image-based tasks, making them ideal for signature analysis. The layers of a CNN learn hierarchical representations of features, enabling the system to automatically identify intricate patterns in signature data. This deep learning approach enhances the adaptability of the system and improves accuracy in distinguishing genuine from forged signatures.

- **Deep Dive into Convolutional Neural Networks (CNNs):**
  CNNs have proven to be instrumental in various image recognition tasks, and their application in signature verification is no exception. The architecture of a CNN comprises convolutional layers, pooling layers, and fully connected layers. The convolutional layers detect local patterns, while pooling layers down sample the input, reducing computational complexity. Fully connected layers then use these learned features to make predictions. The use of CNNs in signature verification leverages their ability to analyze spatial data efficiently, making them adept at classifying and comparing signature images.

- **Overcoming Limitations with ResNet Architecture:**
  The introduction of the ResNet (Residual Network) architecture addresses limitations in training deep neural networks. Traditional CNNs faced challenges as the network depth increased due to vanishing or exploding gradients. ResNet introduces residual blocks, allowing for the creation of deeper and more accurate networks. This innovation has a direct impact on reducing image errors in deep CNNs, contributing to improved overall system performance.

II. RELATED WORK

Signature verification has been a subject of extensive research, with various methodologies and approaches contributing to the advancement of this critical field. One notable avenue of investigation involves the traditional methods of signature authentication. Early systems often relied on manual verification, where experts compared signatures visually. However, the limitations of this approach, including subjectivity and susceptibility to human error, prompted the exploration of automated methods. In recent years, the integration of machine learning and artificial intelligence (AI) techniques has revolutionized signature verification systems. Notably, researchers have explored the application of Support Vector Machines (SVM) for classification tasks in signature verification. SVMs, known for their effectiveness in binary classification, have been employed to distinguish between genuine and forged signatures based on extracted features. Additionally, the adoption of deep learning models, especially Convolutional Neural Networks (CNNs), has gained prominence in signature verification research. CNNs, originally designed for image processing, have demonstrated superior performance in analyzing spatial data, making them well-suited for signature recognition. Researchers have leveraged CNN architectures to enhance the accuracy and efficiency of signature verification systems. Comparative studies have been conducted to evaluate the effectiveness of different CNN models, shedding light on their relative strengths and weaknesses. Another significant area of related work involves the exploration of diverse datasets for training and evaluating signature verification systems. The MCYT Signature Dataset has been widely utilized, featuring a substantial number of signatures with demographic information, allowing researchers to investigate potential correlations between age, gender, and signature characteristics. Furthermore, the inclusion of the GPDS Signature Dataset, which introduces signatures expressed during Greek Sign Language communication, adds a unique linguistic context to the related research landscape. Ethical considerations have not been overlooked in the related work, with scholars addressing concerns related to privacy and consent in signature verification research. Ensuring that datasets used are ethically sourced and that individuals contributing signatures provide informed consent has become an integral aspect of responsible research practices. In conclusion, the related work in signature verification spans traditional manual methods to state-of-the-art machine learning techniques, with a notable shift towards the integration of deep learning models. Diverse datasets and ethical considerations further shape the landscape, contributing to a holistic understanding of the advancements, challenges, and ethical implications within the realm of signature verification research.

III. PROPOSED ARCHITECTURE OVERVIEW

The proposed architecture uses two signatures (real and fake) to train the algorithm. The SV module does the classification work by checking whether two names are the same. If the signature is not verified, it will be considered original authorization and will not be recognized. Our policy recognizes that security breaches may occur, so users are given the opportunity to ensure that their password information is correct. The metrics used to evaluate the program are ERR and accuracy (%). CNN architecture has two main components: extraction and classification. The extraction process takes information from previous layers as input and transfers the features extracted from this layer to the next layer. The block diagram of the proposed SV system is shown in Figure 1. Each mode is explained below:

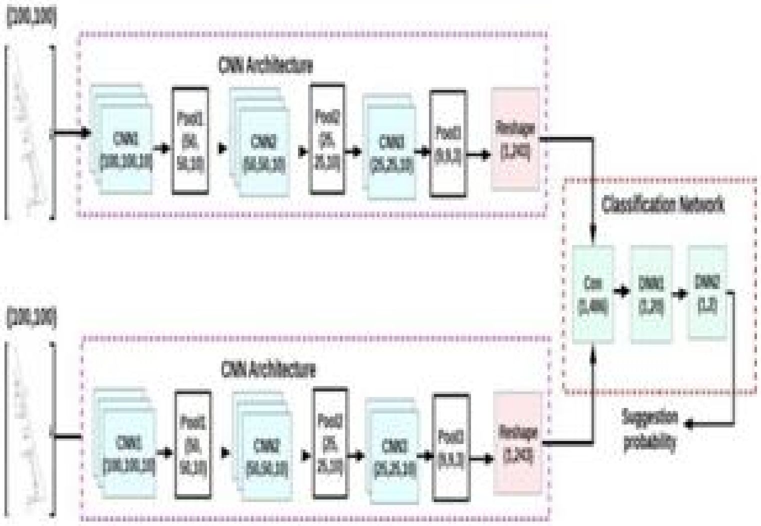

Figure 1: proposed CNN Architecture

Feature Extraction First, threshold α is used to transform the image signature into a binary image (a digital image with only two possible values for each pixel), which helps determine the hue of the image's signature. Then resize the image to 100x 100 to control the size of the features. Finally, this preview image is the SV of the website. Given two signature images, we pass these images to the CNN architecture (shown in the block diagram), which converts 100x100 binary images into 243 dimensional vectors. Our assumption is that the vectors of two images are the same as long as the signature is from the same person. Therefore, two 243dimensional vectors are combined to create a 486dimensional vector, which is then passed through the distribution to create the final result.

- **Three-Layer CNN Architecture**

The design consists of three CNN layers: convolution layer, maximum pooling layer, and layer layer, as described below; various digital signatures have been examined in previous studies. For example, Diaz et al. This is true. A system that can identify signatures using signature models obtained from parallel data and machine learning techniques has been developed. Another work uses Hidden Markov Models (HMM) to demonstrate GPUbased offline signature detection capabilities. There is also research focusing on the creation of proofconcept signatures, such as the creation of pen products. Although early research has developed some methods for digital signature verification, it is worth noting that most of these studies focus on digital signature verification. This work requires the use of a special tool to record the signature pattern. You can expect users to report directly from dedicated devices rather than using this signing certificate. In addition, the methods developed by previous studies have not been abandoned but have been accepted online; This means that a lot of time and resources need to be spent on different parts of the organization. Considering this fact, the ability of the system to sign certificates without trusting these organizations is essential for validating existing certificates and resolving problems that arise in insurance coverage. This research aims to develop a cloud recognition system (CNN) based on neural network algorithms. This will help eliminate forged signatures. Their main goal is to create a picture that illustrates the vision; prepare for maintenance through preregistration and signature; Sign the certificate of completion of the CNN InceptionResNet architecture; and test the accuracy of the application through machine learning. Once completed, it is recommended for use by banks that need to sign certain types of financial transactions to provide additional security. This type of signature verification allows you to verify information to ensure that the signature cannot be forged. Minimize signature and document rejection. Please note that this study will focus on document analysis and signatures that meet academic restrictions and conditions. Additionally, because research and application are based on the neural network model, the results of the system are determined by the data used to inform the model. The nature of machine learning algorithms is that machine learning is also intended to allow for the possibility of unexpected outcomes.

- **Convolutional layer**

This layer is responsible for convolving the feature map of the previous layer with a kernel (such as Gabor or Gaussian). The output of the convolution kernel passes through functions such as hyperbolictangent, sigmoid, softmax and smooth linear function. Mathematically, the convolution process can be expressed as:

$$yja = f(\Sigma i \ SON \ M \ j \ xit- \ 1ktij \ btj) \qquad -1$$

In Equation 1, yja signifies the outcome of the immediate process associated with it, which was previously denoted as xit-1 in earlier systems. Among these components, ktij represents the initial value of the current layer, and btj denotes the variable value of the current layer. Mj represents the chosen value from the input map. The specification is formulated by comparing the value of Mj with the default value.

- **Sampling layer**

This layer's purpose is to reduce the image resolution through down sampling. The input and output mode properties remain constant throughout this operation. As Equation 2 employs low values in the sub sampling function, it mathematically demonstrates that the size of the output map is diminished compared to the sub sampling mask.

$$Y \ t \ j = f(\beta tjdown(xjt1) \ btj) \qquad -2$$

The subsequent function computes n x n map tiles and performs sub sampling using the majority of n x n values within each block area. The nonlinearity or linear activation results in a reduction in the amplitude of the output signal by a factor of n.

- **CNN Architecture**

a) CNN1: Constituting the initial layer in the CNN architecture, its primary role is signature generation and enhancement of image quality. With 13 convolutional layers, encompassing 2 upper and 2 max-pooling layers, CNN1 employs 2 x 2 kernels and 2 x 2 max-pooling layers. The use of two max-pooling layers reduces the feature map dimensions to 50 x 50 x 10. ReLU activation functions characterize the convolutional process.

b) CNN2: As the second layer in the CNN architecture, CNN2 is nonlinear with 2 x 2 cores, reducing its size to 2 x 2. It incorporates a maximum of 2 fully connected layers. Subsequent max-pooling operations further diminish the image dimensions (25, 25, 10), utilizing ReLU activation.

c) CNN3: Representing the third layer in the CNN architecture, CNN3 operates with (3 x 3) image quality, further reducing the output image to (9, 9, 3). The output of CNN3 is resized to match each signature's dimensions (1243). The sigmoid function is employed as the activation function for this layer.

- **Classification**

The classification network converts the ultimate 486-dimensional vector into a two-dimensional vector by amalgamating outcomes from two CNN architecture networks to yield binary results. Initially, the 486-dimensional vector undergoes a Relu transformation within the deep neural network (DNN1), resulting in a 20-dimensional vector. DNN2 then initializes this 20-dimensional vector using the Softmax recognition coefficients. The Softmax function, employed for calculating event probabilities within a group, determines the outcomes for a particular group within a potential set.

IV. METHODOLOGY

In this project, the focal point is the meticulous examination of signature verification, a critical element in the domain of biometric authentication systems. The exploration centers on two pivotal datasets: the MCYT (MasterCard Young Teenager) Signature Dataset and the GPDS (Greek Sign Language Recognition) Signature Dataset. The MCYT dataset, a comprehensive collection of 6600 signature samples, intricately balances 3300 genuine and 3300 forgery signatures from 330 individuals. Its strength lies in capturing diverse writing styles under varied conditions, enhanced by the inclusion of demographic information for potential nuanced analyses. In parallel, the GPDS dataset, comprising 4000 signatures, introduces a unique challenge by featuring signatures expressed during Greek Sign Language communication. This dataset not only provides 2000 genuine and 2000 forgery samples but also introduces dynamic signing variations, offering a distinctive linguistic context. Both datasets collectively form the bedrock for evaluating the adaptability and accuracy of the signature verification system. The MCYT dataset, with its substantial size and variability, stands as a benchmark for real-world conditions. The signatures within this dataset span a spectrum of writing styles and are captured using diverse devices, introducing the necessary complexity for training and evaluating a robust signature verification system. The inclusion of demographic information further enriches the dataset, enabling potential analyses to explore correlations between age, gender, and signature characteristics. In contrast, the GPDS dataset brings a unique and challenging perspective to the project. Signatures captured during Greek Sign Language communication pose a distinctive challenge, introducing dynamic signing variations that go beyond traditional signature dynamics. The dataset's linguistic context adds an extra layer of complexity, making it an ideal source for evaluating the adaptability of signature verification systems in diverse communication scenarios. The significance of these datasets is underscored by their collective contribution to the project's overarching goals. The MCYT dataset mirrors the variability encountered in real-world scenarios, ensuring that the signature verification system is robust enough to handle the intricacies of everyday use. Meanwhile, the GPDS dataset introduces a novel challenge, expanding the system's scope to encompass linguistic nuances and dynamic signing elements. In conclusion, the MCYT and GPDS Signature Datasets serve as integral components in the evaluation and development of the signature verification system. Their respective characteristics, from variability and demographic information to linguistic context and dynamic signing variations, collectively enhance the project's depth and applicability. The insights gained from the analysis of these datasets not only contribute to the advancement of signature verification technology but also underscore the system's adaptability in diverse and evolving communication scenarios.

V. SIMULATION PARAMETERS

We consider two experiments to evaluate the performance of the proposed network compared to the baseline. First, we train the network using different signatures of different people. In Part 2, we continue training with real and fake signatures. The experiment evaluated two conditions using (i) variable names (SV) and (ii) true and false symbols (FS). In this case: (1) in a data store (training and testing are done in the same data store) and (2) in the store data store (training and evaluation are done differently in the same data store). We use the equivalent error rate (EER) as our performance metric. This is as wrong as it is untrue

VI. PROPOSED METHODS& RESULT

In the field of offline signature verification, the authors found a classification system that is sufficient to identify user signatures using limited information during training (fake images containing approximately 9 real images and binary random images). CNNs have proven successful in machine learning-based image processing. CNNs have a very good performance in selecting from the image by finding the filter along with the 2D matrix around the image. The following steps must be completed and executed before images can be entered for training.

- **Image pre-processing:** Image capture and resizing: Save the image pre-processing is a critical step in signature verification systems, playing a pivotal role in enhancing the quality and reliability of the subsequent analysis. This initial phase is designed to address various challenges inherent in signature images, ensuring that the data fed into the verification algorithm is optimized for accurate results.
- **Grayscale scaling:** Grayscale conversion is a fundamental image pre-processing step in signature verification systems, essential for simplifying data representation and reducing computational complexity. This technique involves transforming color images into grayscale, where each pixel is represented by a single intensity value, typically ranging from 0 (black) to 255 (white). The importance of grayscale conversion lies in streamlining subsequent analysis and feature extraction processes while retaining crucial signature information. While grayscale conversion simplifies the representation of signature images, it is important to note that the effectiveness of this step depends on the specific requirements of the signature verification system and the characteristics of the dataset. In cases where color information is deemed crucial, alternative strategies such as color normalization or multispectral analysis may be explored.

- In conclusion, grayscale conversion stands as a fundamental image pre-processing technique in signature verification, striking a balance between data simplification and information retention. By focusing on luminance values, this step optimizes the subsequent stages of the verification system, contributing to enhanced accuracy and efficiency in the authentication process. In signature images, color information may not be as relevant as texture and intensity variations. Grayscale conversion simplifies the image data, focusing on luminance rather than color, which is especially advantageous when dealing with signatures captured in various lighting conditions or with different writing tools.

Navigate to the specific link located at the lower edge (long side) of the image. This action will align the coordinates, effectively dividing the image into (left, top) and (right, bottom). Proceed to fill the image from the edges as needed to create a square format without compromising the integrity of the signature within the image.

VII. CONCLUSION

Error rates compared to traditional CNN architectures. The integration of DSP techniques enhances the analysis of captured images, contributing to the system's robustness in handling various signature styles. Cloud GPU utilization is a key aspect of this project, providing a substantial boost to model training performance, especially with powerful models like RTX 2060. The combination of Python programming and cloud GPU infrastructure facilitates a seamless and efficient development process. The block diagram illustrating hardware components, with the Raspberry Pi at its core, showcases a well-integrated system. The LCD screen displaying signed certificates adds a user-friendly interface, allowing users to quickly ascertain the validity of signatures. The calculation of FAR and FRR, alongside overall accuracy, provides a comprehensive evaluation of the system's functionality. This project not only contributes to the advancement of signature verification technology but also aligns with broader discussions about the future implications of climate change. The focus on cloud-based solutions and efficient GPU utilization reflects a commitment to sustainable practices and the exploration of environmentally friendly technologies. In conclusion, the results highlight the success of the signature verification system, particularly in offline scenarios. The discussion underscores the significance of the ResNet architecture, DSP techniques, and cloud GPU utilization in enhancing the system's accuracy and efficiency. This project not only addresses the immediate need for reliable signature verification but also positions itself as a forward-looking initiative with considerations for environmental impact and sustainability..

REFERENCES

[1]. Jain, A. K., Ross, A., & Prabhakar, S. (2004). "An introduction to biometric recognition."
[2]. Ratha, N. K., Chen, S., & Bolle, R. M. (2001). "Cancelable biometrics: A case study in fingerprints."
[3]. Bromley, J., Bentz, J. W., Bottou, L., Guyon, I., LeCun, Y., Moore, C., ... &Säckinger, E. (1994). "Signature verification using a" siamese" time delay neural network."
[4]. Monadjemi, A. H., & Srinivasan, H. (1994). "Off-line signature verification by a neural network."
[5]. Gonzalez, R. C., & Woods, R. E. (2008). "Digital image processing."
[6]. Pratt, W. K. (2007). "Digital image processing: PIKS Scientific inside."
[7]. Lamel, L., Gauvain, J.-L., & Adda, G. (1986). "Speaker independent speaker verification using Hidden Markov Models."
[8]. Plamondon, R., & Srihari, S. N. (2000). "Online and off-line handwriting recognition: A comprehensive survey."
[9]. Shafait, F., Keysers, D., &Breuel, T. M. (2008). "Pixel-based skin color detection and adaptive thresholding."
[10]. Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, I., &Salakhutdinov, R. R. (2012). "Improving neural networks by preventing co-adaptation of feature detectors."
[11]. Simonyan, K., & Zisserman, A. (2014). "Very deep convolutional networks for large-scale image recognition."
[12]. Lecun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). "Gradient-based learning applied to document recognition."
[13]. Schmidhuber, J. (2015). "Deep learning in neural networks: An overview."
[14]. Lecun, Y., Bengio, Y., & Hinton, G. (2015). "Deep learning."
[15]. Hochreiter, S., &Schmidhuber, J. (1997). "Long short-term memory."
[16]. Kingma, D. P., & Ba, J. (2014). "Adam: A method for stochastic optimization."
[17]. Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). "Deep learning."
[18]. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., &Wojna, Z. (2016). "Rethinking the inception architecture for computer vision."
[19]. Zeiler, M. D., & Fergus, R. (2014). "Visualizing and understanding convolutional networks."
[20]. Ammar, M., &Raveaux, R. (2015). "Offline signature verification: Literature review."